Indice

1. NUOVI SOCI

Durante l'ultimo mese hanno aderito al CLUSIT le seguenti organizzazioni:

- NET Active (Parma),
- RS Advanced Systems (Parma),
- STEP (Roma).

2. GLI ISP DICHIARANO GUERRA ALLO SPAM

Gli Internet Service Providers, principalmente inglesi, ma anche asiatici ed americani, hanno adottato un codice di comportamento particolarmente severo nei confronti delle società di e-commerce che dovessero ricorrere ad azioni di spamming. (http://www.linx.net/press/releases/103.thtml)

150 ISP si sono riuniti il 18 agosto in occasione di un'assemblea generale del London Internet Exchange (LINX). Si tratta dell'organismo che gestisce uno dei principali nodi di interconnessione in Inghilterra, attraverso il quale passa più del 90% del traffico internet nazionale (http://www.linx.net/members/index.thtml). È stato deciso di bloccare l'accesso a quelle società che hanno un sito vetrina "rispettabile" presso un ISP, ma che utilizzano nel contempo un'altro ISP per azioni di SPAM.

Tali misure potranno essere efficaci solo se saranno adottate a livello internazionale e se altri organismi che gestiscono nodi di interconnessione, quali l'Euro-IX o la rete IP europea (RIPE), seguiranno l'esempio del LINX, che chiederà un intervento in tal senso anche al governo inglese e all'OCSE.

3. COMPUTER CRIME - PHISHING

Il laboratorio Anssaif sul Phishing segnala che nello scorso mese di agosto sono pervenute alcune email indirizzate a residenti italiani, ma riguardanti i loro rapporti con una grande banca internazionale americana.

Una ricerca più approfondita, ha soltanto permesso di accertare che i destinatari erano abbonati ad un sito statunitense fornitore di notizie finanziarie.

Le email contenevano un invito a connettersi al sito della banca (naturalmente "fasullo", ma in tutto e per tutto uguale a quello originale) per ricevere gratuitamente istruzioni per una migliore sicurezza nelle operazioni di acquisto su Internet. Per fare ciò, veniva chiesto di fornire i propri dati personali.

Ciò al momento conferma l'assenza di attacchi di questo tipo a clienti italiani di banche italiane.

Sul fronte dell'andamento in generale del fenomeno, ultimamente si sono avuti negli USA circa 250.000 email riguardanti questa tipologia di attacco nel mese di luglio; a tale ritmo, si hanno volumi paragonabili a quelli avvenuti in occasione di attacchi di noti virus (Code Red, NIMDA, Slammer).

Inoltre, il Gruppo Anti Phishing (APWG), costituito come noto da 400 aziende, fra le quali le maggiori banche americane, segnala che il tasso di crescita del numero di attacchi è attorno al 50% al mese.

Al momento sono attaccati i clienti delle banche inglesi, americane ed australiane.

http://www.infoworld.com/article/04/08/04/HNphishingattacks_1.html

I danni sono al momento stimati in oltre 400.000.000 US$, senza considerare la perdita di immagine e di clienti subita dalle banche colpite.

http://www.finextra.com/fullstory.asp?id=12173

Tra le nuove modalità di attacco, si segnalano quattro casi di un certo interesse.

Il primo, si presenta come una possibile fonte di finanziamento per credito personale. Se l'interessato inserisce alcune informazioni che lo riguardano, e necessarie per costruire il profilo di rischio del soggetto, il sito restituisce adeguate informazioni sulla possibilità di ottenere prestiti personali.

E' chiaro che così facendo, il soggetto dà delle informazioni che possono essere utilizzate sia per essere rivendute, sia per portare attacchi di phishing o per compiere frodi.

Una domanda potrebbe sorgere spontanea: nessuno è così sciocco (si spera) da dare il proprio nome ed indirizzo! E' vero, ma non occorre essere grandi esperti per sapere che il pc di ognuno di noi contiene molte informazioni quali: a chi è intestata la licenza di un software; chi per default è l'autore dei documenti Word (contenuto in Proprietà); ecc. Non è quindi eccessivamente difficile (Su questo tema delle informazioni contenute in un qualsiasi computer e su come ottenerle, il nostro laboratorio metterà presto a disposizione nella pagina "White papers" una specifica e dettagliata nota tecnica)

Per maggiori informazioni sulla notizia data:

http://www.oswegodailynews.com/yourmoneyarticle.asp?id=46706&section=yourmoney&network=oswego

Il secondo caso riguarda il sempre maggior uso dei banner pubblicitari quale veicolo per l'inserimento di trojan e "malware" sui computer.

Per maggiori informazioni:

http://news.netcraft.com/archives/2004/08/06/phishing_attacks_using_banner_ads_to_spread_malware.html

Il terzo caso che riportiamo, riguarda un avviso della banca irlandese AIB che ha avvertito i suoi clienti che potrebbe apparire, mentre operano in rete, un loro presunto invito a fornire dei dati personali (in allegato abbiamo riportato la pagina web della AIB con l'avviso).

E' il classico caso di phishing, ma ciò che "stuzzica" l'interesse è che questo messaggio appariva anche quando l'utente era collegato con il servizio di home banking ufficiale della AIB.

Si possono fare diverse ipotesi, ma l'ideale sarebbe poter avere maggiori dettagli, onde capire se vi è stata una nuova modalità e quale.Ci stiamo interessando con la polizia per avere tali informazioni.

Il quarto caso, riguarda un attacco attualmente in corso e diretto a non residenti negli Stati Uniti, non cittadini americani, possessori di una casa negli USA.

A questi perviene una presunta lettera dall'ufficio delle tasse (IRS) con un modulo da compilare (IRS Form W-8BEN, "Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding,") qualora vogliano evitare di pagare l'aliquota massima sulla proprietà. Il modulo prevede la dichiarazione di dati personali, atti successivamente a perpetrare azioni fraudolente a carico dell'ignaro dichiarante.

Dato che l'argomento tasse è un tema che trova tutti molto sensibilizzati, l'"esca" è davvero allettante!

Per maggiori informazioni:

http://www.webcpa.com/WebCPA/index.cfm/txtFuse/dspShellContent/fuseAction/DISPLAY/numContentID/53443/numSiteID/12/numTaxonomyTypeID/10/numTaxonomyID/937.htm

Il caso precedente non avrebbe nulla di particolare (Totò e soci ci hanno abituato a ben più sofisticati sistemi per ingannare gli ingenui!) se non fosse che le lettere e le email vengono sempre più indirizzate ai corretti destinatari.

Ciò vuol dire una cosa sola: i criminali riescono ad avere le informazioni giuste.

A questo proposito, di un certo interesse è la notizia che una ricerca con il motore Google ha permesso di individuare possessori di carte di credito con riferimenti personali, fra i quali anche il numero della carta.

Malgrado fosse stato riferito che i numeri erano obsoleti, alcune persone, contattate direttamente, avrebbero confermato la qualità dell'informazione.

Siccome non è la prima volta che informazioni trovate in rete sono servite per un attacco, e dato che non possiamo pensare che si sia trattato di una scelta voluta, non possiamo che dedurne che, a meno di una alquanto rara disattenzione o ingenuità, si sia trattato di un'apertura inaspettata di un server al mondo esterno.

Appare quindi sempre più necessario che nelle nostre aziende, se ancora non fatto,

- classifichiamo le informazioni in base alla riservatezza,

- teniamo sotto controllo quali informazioni sono in rete, e

- ci accertiamo non siano tali da poter fornire informazioni utili ad eventuali criminali (nel qual caso le inseriamo fra quelle dichiarate riservate e quindi non divulgabili).

In particolare, dobbiamo fare attenzione che quando ci sono delle modifiche alle applicazioni Web, non si creino delle "aperture" non volute, sfruttabili queste da hacker per accedere all'interno di uno o più server.

Sottolineiamo questo possibile attacco in quanto non molto tempo fa, nel corso del periodico "vulnerability assessment" operato da una Società specializzata, è stata accertata questa debolezza presso un nostro associato che ha il sito gestito in outsourcing; chiaramente gli sviluppatori della Società sono caduti dalle nuvole! (Qui si porrebbe il problema dell'outsourcing e delle relative clausole contrattuali che, nella fattispecie, qualora fosse stato un hacker ad impadronirsi del server, non avrebbero coperto il possibile danno reputazionale, legale ed operativo subito dalla banca).

Ma su questo problema ci ritorneremo prossimamente.

Per maggiori informazioni sull'episodio che ha interessato Google consultare:

http://news.com.com/2100-1029-5295661.html

A titolo di curiosità, a proposito di eccessive informazioni in rete, citiamo un articolo nel quale si riporta che il Dipartimento di Home Security ha trovato sul Web descrizioni particolareggiate, e anche tridimensionali, degli edifici di aziende americane, possibili obiettivi terroristici in New York. Fra questi casi, Citygroup, noto obiettivo, ha anche riportato sufficienti informazioni atte ad indicare un punto debole nella struttura di sostegno dell'intero edificio.

Le aziende sono state invitate cortesemente a non aiutare i terroristi.

http://www.computerworld.com/securitytopics/security/story/0,10801,95108,00.html

***Fonte**: ANSSAIF - Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria*

4. SEMINARIO CLUSIT Voice-over-IP

In settembre riprende il ciclo dei Seminari Clusit.

Sono aperte le iscrizioni (gratuite per i Soci)* al 2° seminario "Voice-over-IP", che si terrà il 21 settembre a Milano allo StarHotel Splendido in Viale Andrea Doria, 4.

PROGRAMMA

Introduzione alla VoIP

Considerazioni su QoS

Protocolli Voce:

- H.323
- SIP
- Gateway decomposition

Considerazioni di sicurezza:

- Address translation
- Firewall
- Cifratura IPSec e cifratura alternativa
- Rischi, minacce e vulnerabilitá generiche

Considerazioni sul deployment, disponibilitá, integrazione, gestione e monitoraggio:

- Convergenza ed IP Telephony: scenari e ruoli tecnologici
- Architetture disponibili: pro e contro
- IP Telephony: i punti di controllo
- Percorsi e problematiche della migrazione

Conslusioni, Q&A

AGENDA

Registrazione: 13,50

Inizio Seminario: 14,10

Fine lavori: 18,10

Docenti: Stefano Bodini, Marco Misitano

*Condizioni e modalità di iscrizione per Soci e non soci su www.clusit.it/edu

Per ogni informazione chiedere a edu@clusit.it

5. ULTIMO SEMINARIO CISSP del 2004 in Italia

La settimana dal 11 al 15 ottobre 2004 è l'ultima opportunità di quest'anno per frequentare il seminario CISSP in Italia.

Avrà luogo a Milano e farà seguito l'esame il 20 novembre.

Il 25 settembre è l'ultimo giorno per iscriversi al seminario ad un prezzo agevolato.

Tutte le informazioni sui corsi e sugli esami in Italia sono su www.clusit.it/isc2.

Per ogni altra informazione inviare una e-mail a isc2@clusit.it

6. EVENTI SICUREZZA (Tutti i dettagli sulle manifestazioni sono disponibili sul sito CLUSIT alla voce EVENTI)

21 settembre 2004, Milano
SEMINARIO CLUSIT - "Voice-over-IP"

7-8 ottobre 2004, Milano
IBM Global Security Conference III

7-8 ottobre 2004, Ginevra
"Homeland Security Forum - The United States, Europe and Beyond: New Challenges for Institutions and the Private Sector"

11-15 ottobre 2004, Milano
Seminario di preparazione all'esame CISSP

12 ottobre 2004, Roma
SEMINARIO CLUSIT - "Voice-over-IP"

13 ottobre 2004, Milano
"Facciamo il punto sulla sicurezza"

14 ottobre 2004, Milano
"La banca aperta - Business continuity e sicurezza nella banca multicanale" Conferenza organizzata da AZIENDA BANCA (edipi), in collaborazione con ANSSAIF e CLUSIT

19 ottobre 2004, Milano
SEMINARIO CLUSIT - "Documento Elettronico"

21-25 ottobre, Fiera di Milano
SMAU

29 ottobre, Roma EUR (nell'ambito del Salone "Prevenzione Italia")
Convegni CLUSIT
mattino: "Il management delle informazioni in azienda: Sicurezza e Privacy"
pomeriggio: "Sicurezza informatica e tutela dei dati personali in ambito sanitario: quali misure stanno adottando le strutture ospedaliere italiane"

CLUSIT - ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA*
Dipartimento di Informatica e Comunicazione - Università degli Studi di Milano
Via Comelico 39 - 20135 MILANO - cell. 347.2319285
* associazione senza fini di lucro, costituita il 4 luglio 2000